# INSTALL AND UNINSTALL CONTROLLER WITH SECURITY CHECK FUNCTION AND ITS METHOD

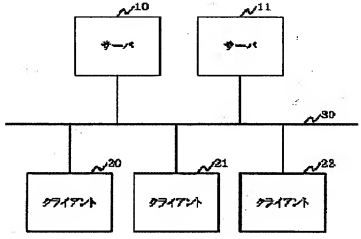

| | |
|---|---|
| **Patent number:** | JP2000339142 |
| **Publication date:** | 2000-12-08 |
| **Inventor:** | CHIBANA KAORU; YONAMINE ISAO |
| **Applicant:** | NEC SOFTWARE OKINAWA LTD |
| **Classification:** | |
| **- international:** | G06F9/06 |
| **- european:** | |
| **Application number:** | JP19990149440 19990528 |
| **Priority number(s):** | |



Abstract of **JP2000339142**

PROBLEM TO BE SOLVED: To prevent a misoperation due to any malicious illegal operation or a fault, and to further safely realize the install and uninstall of an application by checking the security of an executer at the time of operating the install and uninstall of the application.

SOLUTION: This device is composed of a sever 10 which security-checks whether or not a request for the permission of the install and uninstall of an application is proper, a server 11 which substitutes for the server 10 when the server 10 breaks down, clients 20, 21, and 22 which request the permission of the install and uninstall of the application, a storage device 100 which stores data necessary for the processing of the server, and a network cable 30 for connecting each server 10 and 11 with each client 20-22.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開2000-339142

（Ｐ２０００－３３９１４２Ａ）

(43)公開日　平成12年12月8日(2000.12.8)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　9/06 | ４１０ | Ｇ０６Ｆ　9/06 | ４１０Ｂ | 5B076 |
| | ５５０ | | ５５０Ｚ | |

審査請求　有　請求項の数15　ＯＬ（全 14 頁）

(21)出願番号　特願平11-149440

(22)出願日　平成11年5月28日(1999.5.28)

(71)出願人　000123262
沖縄日本電気ソフトウェア株式会社
沖縄県那覇市久米2丁目3番15号

(72)発明者　知花　薫
沖縄県那覇市久米2丁目3番15号　沖縄日本電気ソフトウェア株式会社内

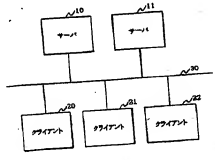
(72)発明者　與那嶺　勲
沖縄県那覇市久米2丁目3番15号　沖縄日本電気ソフトウェア株式会社内

(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム（参考）　5B076 AA01 AA11 FA06 FB11

(54)【発明の名称】セキュリティチェック機能付きインストール及びアンインストール制御装置と方法

(57)【要約】
【課題】実行者のセキュリティがチェックされないために、誰もがアプリケーションのインストール及びアンインストールを実行できてしまう。
【解決手段】アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバ１０、サーバ１０が故障した際にその代理を行うサーバ１１、アプリケーションのインストール及びアンインストールの許可要求をするクライアント２０、２１、２２、サーバの処理に必要なデータを蓄積している記憶装置１００、及び各サーバと各クライアントを結ぶネットワークケーブル３０から構成し、アプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、悪意を持った不正操作や過失による誤操作を防ぎ、より安全にアプリケーションのインストール及びアンインストールを行う。



1

【特許請求の範囲】

【請求項1】　アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうか許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項2】　アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項3】　クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を

2

検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するものなのかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データをデータ生成部の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名か

らの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項４】　処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させることを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項５】　処理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置



よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御装置。

【請求項６】　アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうか許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項７】　アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御

し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項８】　クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するものなのかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加され、履歴情報を付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。



【請求項９】　処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケ

ーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させることを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項１０】　処理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了することを特徴とするセキュリティチェック機能付きインストール及びアンインストール制御方法。

【請求項１１】　アプリケーションのインストール及びアンインストールをクライアントで実行時、アプリケーションのインストール及びアンインストール開始状態であることをクライアントのオペレーティングシステムが検知し、アプリケーションのインストール及びアンインストールを一時停止状態した後サーバへアプリケーションのインストール及びアンインストールの許可要求し、サーバは各クライアントからの許可要求が妥当なものかどうか許可要求と同時に送られたログオンユーザ名及びパスワードの含まれた許可要求データを元にセキュリティチェックを行い、正常な操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当であるとセキュリティチェックで判断し、各クライアントへ実行許可を通知し、各クライアントは通知を受け取った後、アプリケーションのインストール及びアンインストールを継続し、悪意を持った不正操作や過失による誤操作が行われた場合は、サーバはアプリケーションのインストール及びアンインストールの許可要求が妥当でないとセキュリティチェックで判断し、各クライアントへ実行拒否を通知し、各クライアントでは通知を受け取った後、アプリケーションのインストール及びアンインストールを中止する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項１２】　アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバと、アプリケーションのインストール及びアンインストールの許可要求をするクライアントと、クライアントとサーバの処理に必要なデータを蓄積している記憶装置と、サーバと各クライアントを結ぶネットワークケーブルから構成し、サーバは、クライアントから送信された許可要求データを処理するデータ生成部と、データ制御部、データ検証部を備え、データ



生成部は、復号生成部、暗号生成部、認証生成部からなり、復号生成部は、暗号化されたデータをデータ検証部で処理できるように復号化し、暗号生成部は、復号化されたデータを記憶装置で保管できるように暗号化し、認証生成部は、復号生成部で復号化されたデータからデータ検証部で検証するためのデータを生成し、データ制御部は、クライアント、データ生成部、データ制御部、データ検証部、記憶装置を行き交うデータの流れを制御し、データ検証部は、クライアントより送られた許可要求データが妥当なものであるかを検証する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項１３】　クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するものなのかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないかを判断し、不正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証

9

データをデータ生成の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続すること、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項１４】　処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許

10

可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させる処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【請求項１５】　処理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了する処理をコンピュータに実行させるためのプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はセキュリティチェック機能付きインストール及びアンインストール制御装置と方法に関し、特にアプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、より安全にアプリケーションのインストール及びアンインストールを行うセキュリティチェック機能付きインストール及びアンインストール制御装置と方法に関する。

【０００２】

【従来の技術】従来、アプリケーションのインストール及びアンインストールにおいてのセキュリティチェックは、アプリケーションのＣＤ－ＲＯＭやマニュアルに記載されているＩＤを入力することで、インストール及びアンインストールプログラムがＩＤチェックを行っていた。

【０００３】

【発明が解決しようとする課題】上述した従来のセキュリティチェック機能付きインストール及びアンインストールは、第１の問題点は、アプリケーションのインストール及びアンインストールを実行する実行者のセキュリティがチェックされないために、誰もがアプリケーションのインストール及びアンインストールを実行できることである。

11

【０００４】その理由は、従来のアプリケーションのインストール及びアンインストールでは実行者のセキュリティチェックは考慮されていないためである。

【０００５】本発明の目的は、アプリケーションのインストール及びアンインストールにおいて実行者のセキュリティをチェックすることにより、悪意を持った不正操作や過失による誤操作を防ぎ、より安全にアプリケーションのインストール及びアンインストールを行うことができるセキュリティチェック機能付きインストール及びアンインストール制御装置と方法を提供するものである。

【０００６】

【課題を解決するための手段】第１の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、クライアントでアプリケーションのインストール及びアンインストールの実行が開始されると、クライアントのオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知し、クライアントのオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアントで現在操作している実行者のデータを暗号化し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとしてサーバへ送信し、サーバは、クライアントから送信された許可要求データをデータ制御部で受信し、データ制御部は、許可要求データをデータ生成部の復号生成部へ送り、復号生成部は、許可要求データを復号化しデータ制御部を介してデータ検証部へ送り、データ制御部は、記憶装置に格納されているインデックスデータを取り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データのクライアントマシン名がネットワークに存在するものなのかをサーバのオペレーティングシステムに問い合わせ、存在するならば、許可要求データのログオンユーザ名またはパスワードと、インデックスデータのログオンユーザ名またはパスワードが一致するものを検索し、同じデータが見つかった場合は、データ制御部がインデックスデータのナンバーをキーとして、記憶装置に格納されている認証データを取り出し、データ生成部の復号生成部へ送り、復号生成部は、認証データを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部では、許可要求データのアプリケーション名、アプリケーションのバージョン情報と、認証データのアプリケーション名、アプリケーションのバージョン情報が一致するものを検索し、同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限情報が実行可能になっているかをチェックし、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断し、不

12

正な要求でない正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データをデータ生成部の認証生成部へ送り、認証生成部は、認証データに正常な操作である旨の正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴情報を付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り、暗号化し、暗号化された認証データはデータ制御部を介して記憶装置へ保管し、データ制御部は認証データが保管された後に、クライアントへアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを送信し、クライアントはサーバより送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを継続することと、また、悪意を持った不正操作や過失による誤操作が行われた場合は、ネットワークに存在しないクライアントマシン名からの不正操作、ログオンユーザ名またはパスワードが不正であることを検出可能にし、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出し、検出されたら認証データをデータ生成の認証生成部へ送り、認証生成部は、認証データに不正な操作である旨の不正操作の原因究明に必要なデータの異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む履歴情報を付加し、履歴が付加された認証データは、データ制御部を介してデータ生成部の暗号生成部へ送り暗号化し、暗号化された認証データは、データ制御部を介して記憶装置へ保管し、データ制御部は認証データデータが保管された後に、クライアントへアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを送信し、クライアントではサーバより送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データを受信し、アプリケーションのインストール及びアンインストールを中止して終了するように構成されている。

【０００７】また、第２の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、処理装置は入力装置と出力装置を備え、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置にキーワード入力画面を表示し、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを作成し、アプリケーションのインストール及びアンインストール許可を要求する許可要求データとして、データ制御部を介してデータ検証部へ送り、同時にデータ制御部は、記憶装置に格納されているインデックスデータを取

り出し、データ生成部の復号生成部へ送り、復号生成部は、インデックスデータを復号化し、データ制御部を介してデータ検証部へ送り、データ検証部は、許可要求データとインデックスデータを比較し、許可要求データが不正なものでないかを判断し、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可通知データを作成し、アプリケーションのインストール及びアンインストール処理を継続する、また、要求データが不正なものであった場合は、アプリケーションのインストール及びアンインストール不許可通知である拒否通知データを作成し、出力装置にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し、アプリケーションのインストール及びアンインストール処理を終了させるように構成されている。

【０００８】また、第３の発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、処理装置は入力装置と出力装置を備え、ファイルの作成及び削除を検知すると、出力装置にキーワード入力画面を表示して、実行者に対して、入力装置よりキーワードを入力させ、マシン名、ユーザ名、パスワード、及びキーワードを含む実行者のデータを暗号化して、ファイルの作成及び削除許可を要求する許可要求データを作成し、また、ファイルの作成及び削除拒否通知データを作成した場合は、出力装置にファイルの作成及び削除の拒否を示すメッセージを表示し、ファイルの作成及び削除処理を終了するように構成されている。

【０００９】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１０】図１は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の一実施の形態を示す接続系統図である。

【００１１】図１を参照すると、本実施の形態は、アプリケーションのインストール及びアンインストールの許可要求が妥当かどうかをセキュリティチェックするサーバ１０、サーバ１０と同等の機能を持ち、サーバ１０が故障した際にその代理を行うサーバ１１、アプリケーションのインストール及びアンインストールの許可要求をするクライアント２０、クライアント２１、クライアント２２、及び各サーバと各クライアントを結ぶネットワークケーブル３０から構成されている。

【００１２】図２は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の一実施の形態を示すブロック図である。

【００１３】図２を参照すると、サーバ１０と、クライアント２０、サーバ１０の処理に必要なデータを蓄積している記憶装置１００からなる。

【００１４】サーバ１０は、クライアント２０から送信された許可要求データを処理するデータ生成部２００



と、データ制御部３００、データ検証部４００を備えている。

【００１５】データ生成部２００は、データ生成方法の違いにより復号生成部２０１、暗号生成部２０２、認証生成部２０３の３つからなる。復号生成部２０１は、暗号化されたデータをデータ検証部４００で処理できるように復号化する。暗号生成部２０２は、復号化されたデータを記憶装置１００で保管できるように暗号化する。認証生成部２０３は、復号生成部２０１で復号化されたデータからデータ検証部４００で検証するためのデータを生成する。

【００１６】データ制御部３００は、クライアント２０、データ生成部２００、データ制御部３００、データ検証部４００、記憶装置１００を行き交うデータの流れを制御する。

【００１７】データ検証部４００は、クライアント２０より送られた許可要求データが妥当なものであるかを検証する。

【００１８】次に、本発明の実施の形態の動作について、図２、図３、図４、及び図５を参照して詳細に説明する。

【００１９】図３は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の実施の形態の動作を示す流れ図であり、図４及び図５は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法のデータの構成を示す構成図である。

【００２０】クライアント２０でアプリケーションのインストール及びアンインストールの実行が開始されると、クライアント２０のオペレーティングシステムがアプリケーションのインストール及びアンインストール開始状態を検知する（図３のステップＡ１）。

【００２１】次に、クライアント２０のオペレーティングシステムでアプリケーションのインストール及びアンインストールを一時停止状態にし、クライアント２０で現在操作している実行者のデータ（クライアントマシン名Ｃ、ログオンユーザ名Ｄ、パスワードＥ、インストール及びアンインストールするアプリケーション名Ｆ、アプリケーションのバージョン情報Ｇ）を暗号化して、アプリケーションのインストール及びアンインストール許可を要求する許可要求データＢ１としてサーバ１０へ送信する（ステップＡ２）。

【００２２】サーバ１０では、クライアント２０から送信された許可要求データＢ１をデータ制御部３００で受信する。データ制御部３００では、許可要求データＢ１をデータ生成部２００の復号生成部２０１へ送る。復号生成部２０１では、許可要求データＢ１を復号化しデータ制御部３００を介してデータ検証部４００へ送る（ステップＡ３）。

【００２３】データ制御部３００では、記憶装置１００

15

に格納されているインデックスデータＢ３を取り出し、データ生成部２００の復号生成部２０１へ送る。復号生成部２０１では、インデックスデータＢ３を復号化し、データ制御部３００を介してデータ検証部４００へ送る。データ検証部４００では、許可要求データＢ１のクライアントマシン名Ｃがネットワークに存在するものなのかをサーバ１０のオペレーティングシステムに問い合わせる。存在するならば、許可要求データＢ１のログオンユーザ名Ｄ／パスワードＥと、インデックスデータＢ３のログオンユーザ名Ｄ／パスワードＥが一致するものを検索（図５のサーチ１）する（ステップＡ４）。

【００２４】同じデータが見つかった場合は、データ制御部３００がインデックスデータＢ３のナンバーＪをキーとして、記憶装置１００に格納されている認証データＢ４（インデックスデータＢ３のナンバーＪをキーとして昇順に並んでいるデータ）を取り出し（サーチ２）、データ生成部２００の復号生成部２０１へ送る。復号生成部２０１では、認証データＢ４を復号化し（ステップＡ５）、データ制御部３００を介してデータ検証部４００へ送る。

【００２５】データ検証部４００では、許可要求データＢ１のアプリケーション名Ｆ、アプリケーションのバージョン情報Ｇと、認証データＢ４のアプリケーション名Ｆ、アプリケーションのバージョン情報Ｇが一致するものを検索（サーチ３）する。

【００２６】同じデータが見つかった場合は、アプリケーションのインストール及びアンインストールの実行権限Ｋ情報（実行可能または実行不可能と記録されている）が実行可能になっているかをチェック、アプリケーションのインストール及びアンインストール許可の要求が不正なものでないか判断する（ステップＡ６）。

【００２７】不正な要求でない、すなわち正当なアプリケーションのインストール及びアンインストール許可の要求であった場合は、認証データＢ４をデータ生成２００の認証生成部２０３へ送る。認証生成部２０３では、認証データＢ４に正常な操作である旨の履歴Ｌ情報を付加する。履歴Ｌ情報には、正常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間を含む。また必要であれば実行権限Ｋ情報の変更も行う。

【００２８】履歴Ｌ情報を付加するのは、不正が行われた場合の原因究明に有効な情報となるためである。履歴Ｌ情報を付加された認証データＢ４は、データ制御部３００を介してデータ生成部２００の暗号生成部２０２へ送り、暗号化する（ステップＡ７）。

【００２９】暗号化された認証データＢ４はデータ制御部３００を介して記憶装置１００へ保管される（ステップＡ８）。

【００３０】データ制御部３００は認証データが保管された後に、クライアント２０へアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データＢ２を送信する（ステップＡ９）。

16

【００３１】クライアント２０ではサーバ１０より送られたアプリケーションのインストール及びアンインストール許可を通知する許可または拒否通知データＢ２を受信し、アプリケーションのインストール及びアンインストールを継続する（ステップＡ１０～Ａ１２）。

【００３２】以上が正常な操作が行われた際の動作である。

【００３３】次に悪意を持った不正操作や過失による誤操作が行われた際の動作は、ステップＡ４または、ステップＡ６で検出される。

【００３４】ステップＡ４では、ネットワークに存在しないクライアントマシン名Ｃからの不正操作、ログオンユーザ名Ｄ／パスワードＥが不正であることが検出可能である。

【００３５】ステップＡ６では、個々のアプリケーションに対して不正なインストール及びアンインストールが要求されたかを検出できる。検出されたら認証データＢ４をデータ生成２００の認証生成部２０３へ送る。認証生成部２０３では、認証データＢ４に不正な操作である旨の履歴Ｌ情報を付加する。履歴Ｌ情報には、不正操作の原因究明に必要なデータ（異常操作、クライアントマシン名、ログオンユーザ名、パスワード、操作が行われた時間）を含む。履歴Ｌが付加された認証データＢ４は、データ制御部３００を介してデータ生成部２００の暗号生成部２０２へ送り暗号化する（ステップＡ１３）。

【００３６】暗号化された認証データＢ４は、データ制御部３００を介して記憶装置１００へ保管する（ステップＡ１４）。

【００３７】データ制御部３００は認証データＢ４データが保管された後に、クライアント２０へアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データＢ２を送信する（ステップＡ１５）。

【００３８】クライアント２０ではサーバ１０より送られたアプリケーションのインストール及びアンインストール拒否を通知する許可または拒否通知データＢ２を受信（ステップＡ１６）し、アプリケーションのインストール及びアンインストールを中止して終了する。

【００３９】本発明の第１の実施の形態では、２つのサーバ、３つのクライアントの場合について説明したが、サーバ、クライアントともに装置の数に制限はない。

【００４０】次に、本発明の第２の実施の形態の動作について、図４、図５、図６、及び図７を参照して詳細に説明する。

【００４１】図６は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第２及び第３の一実施の形態を示すブロック図であ

り、図７は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第２の実施の形態の動作を示す流れ図である。

【００４２】図６を参照すると、本発明の第２の実施の形態は、キーボード等の入力装置１３とディスプレイ装置等の出力装置１２を備える点、実行者のデータ作成時にデータ入力を必要とする点で異なる。

【００４３】本第２の実施の形態の説明では、第１の実施の形態で説明したサーバ／クライアント型の形態ではなく、スタンドアロン型での実施例について説明する。したがって、サーバ１０とクライアント２０のデータのやり取りであるステップＡ２からＡ３、Ａ９からＡ１０、及びＡ１５からＡ１６の処理が不要となり、代わりにデータを作成及び入出力を行うステップＣ１からＣ５の処理が追加となる。

【００４４】図７のステップＡ１からＡ１４で示される本第２の実施の形態は、第１の実施の形態のステップＡ１からＡ１４の動作と同一のため、説明は省略する。なお、本第２の形態では、第１の実施の形態でサーバ１０上で行っていたステップＡ４からＡ８、ステップＡ１３からＡ１４の処理もスタンドアロン型を構成する処理装置１０を含む同一の装置上で行う。

【００４５】第１の実施の形態では、クライアント２０のオペレーティングシステムが、アプリケーションのインストール及びアンインストールの開始を検知した時点で実行者のデータを暗号化して、許可要求データＢ１を送信していた。そのため、クライアント２０が既に起動済みであれば、クライアント２０にログインした本人かどうかを確認する手段がないため、ログインした本人以外が操作した場合でも、インストール及びアンインストールが可能であった。

【００４６】本第２の実施の形態では、オペレーティングシステムがアプリケーションのインストール及びアンインストールの開始を検知すると、出力装置１２にキーワード入力画面を表示して、実行者に対して、入力装置１３よりキーワードＨを入力させ（ステップＣ１）、実行者のデータ（マシン名Ｃ、ユーザ名Ｄ、パスワードＥ、キーワードＨ）を作成して（ステップＣ２）、アプリケーションのインストール及びアンインストール許可を要求する許可要求データＤ１として、データ制御部３００を介してデータ検証部４００へ送る。同時にデータ制御部３００は、記憶装置１００に格納されているインデックスデータＤ２を取り出し、データ生成部２００の復号生成部２０１へ送る。復号生成部２０１では、インデックスデータＤ２を復号化し、データ制御部３００を介してデータ検証部４００へ送る。データ検証部４００では、許可要求データＤ１とインデックスデータＤ２を比較し、許可要求データが不正なものでないかを判断する（ステップＡ６）。

【００４７】本第２の実施の形態においては、正常な要求の場合は、アプリケーションのインストール及びアンインストールの許可または拒否通知データＢ２を作成し（ステップＣ３）、アプリケーションのインストール及びアンインストール処理を継続する（ステップＡ１１～Ａ１２）。



【００４８】一方、要求データが不正なもの（キーワードＨが不一致など）であった場合は、アプリケーションのインストール及びアンインストール不許可通知である許可または拒否通知データＢ２を作成し（ステップＣ４）、出力装置１２にアプリケーションのインストール及びアンインストールの拒否を示すメッセージを表示し（ステップＣ５）、アプリケーションのインストール及びアンインストール処理を終了させる（ステップＡ１２）。

【００４９】次に、本発明の第３の実施の形態の動作について、図８を参照して詳細に説明する。

【００５０】図８は本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第３の実施の形態の動作を示す流れ図である。

【００５１】図８を参照すると、本発明の第３の実施の形態は、第１、または第２の実施の形態とは、第１及び第２の実施の形態が、アプリケーションのインストール及びアンインストールを対象としていたのに対して、本第３の実施の形態ではファイルの作成及び削除が対象となっている点で異なる。したがって、本発明の第３の実施の形態では、図８のステップＡ１がファイルの作成及び削除の開始となり、ステップＡ１１がファイルの作成及び削除の実行、ステップＡ１２が、ファイルの作成及び削除の終了となる。

【００５２】次に、具体例について説明すると、図６に示すシステムでファイルの作成及び削除を検知すると、出力装置１２にキーワード入力画面を表示して、実行者に対して、入力装置１３よりキーワードＨを入力させ（ステップＣ１）、実行者のデータ（マシン名Ｃ、ユーザ名Ｄ、パスワードＥ、キーワードＨ）を暗号化して、ファイルの作成及び削除許可を要求する許可要求データＤ１を作成する（ステップＣ２）。

【００５３】また、ファイルの作成及び削除拒否通知データを作成（ステップＣ４）した場合は、出力装置１２にファイルの作成及び削除の拒否を示すメッセージを表示（ステップＣ５）し、ファイルの作成及び削除処理を終了する（ステップＡ１２）。

【００５４】尚以上のような処理プログラムを記録した記録媒体を有し、コンピュータに実行させることもできる。

【００５５】

【発明の効果】以上説明したように、本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法は、第１の効果は、アプリケーションのインストール及びアンインストールの初期段階、すな

わちファイルの追加または削除が行われる前に、悪意を持った不正操作や過失による誤操作を防げることにある。

【００５６】その理由は、アプリケーションのインストール及びアンインストールの初期段階で不正操作または誤操作が検出できるためである。

【００５７】第２の効果は、決められたアプリケーションのみインストール及びアンインストールを実行することが可能になる。

【００５８】その理由は、クライアントから許可要求データを送信する際に、そのデータにアプリケーション名やバージョン情報などを付加しておくことで、記憶装置にある認証データのインストール及びアンインストール実行権限情報（アプリケーション毎に持つようにする）と比較検証することができるためである。

【図面の簡単な説明】

【図１】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の一実施の形態を示す接続系統図である。

【図２】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の一実施の形態を示すブロック図である。

【図３】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第１の実施の形態の動作を示す流れ図である。

【図４】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法のデータの構成を示す構成図である。

【図５】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法のデータの構成を示す構成図である。

【図６】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第２及び第３の一実施の形態を示すブロック図である。

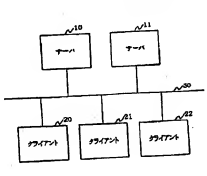
【図７】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第２の実施の形態の動作を示す流れ図である。

【図８】本発明のセキュリティチェック機能付きインストール及びアンインストール制御装置と方法の第３の実施の形態の動作を示す流れ図である。

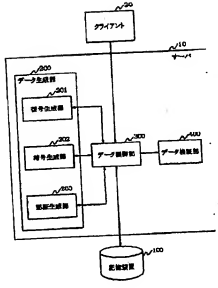
【符号の説明】

１０　サーバ、処理装置
１１　サーバ
１２　出力装置
１３　入力装置
２０，２１，２２　クライアント
３０　ネットワークケーブル
１００　記憶装置
２００　データ生成部
２０１　復号生成部
２０２　暗号生成部
２０３　認証生成部
３００　データ制御部
４００　データ検証部

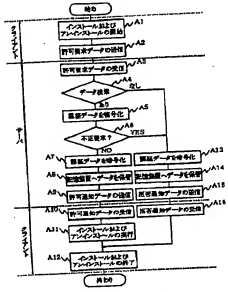
【図１】



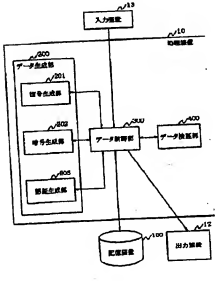
【図２】


クライアント
データ生成部
署名生成部
暗号生成部
認証生成部
データ制御部
データ放送部
記憶装置

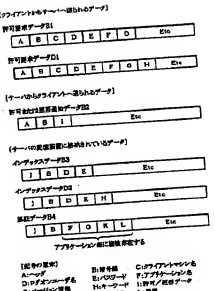
【図３】


始め
インストール及びアンインストールの開始
許可要求データの送信
許可応答データの受信
データ送信
NO
YES
署名データを暗号化
不正検出？
NO
YES
署名データを暗号化
署名データを暗号化
記憶装置へデータを保存
記憶装置からデータを読出
許可追加データの送信
拒否追加データの送信
許可追加データの受信
拒否追加データの受信
インストール又はアンインストールの実行
インストール又はアンインストールの終了
終わり

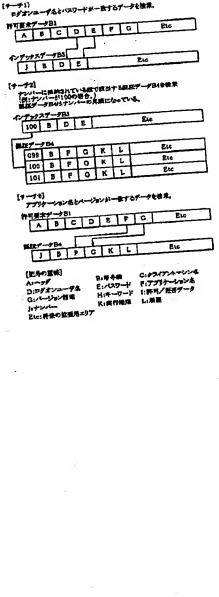
【図６】


入力装置
データ生成部
署名生成部
暗号生成部
認証生成部
データ制御部
データ放送部
記憶装置
出力装置

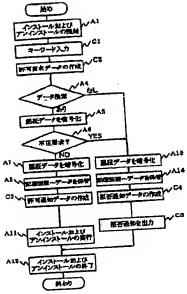
【図４】


[クライアントからサーバーへ送られるデータ]
許可要求データD1
A B C D E F G Etc
許可要求データD1
A B C D E F G H Etc
[サーバからクライアントへ送られるデータ]
許可結果データD2
A B I Etc
[サーバの記憶装置に格納されているデータ]
インデックスデータD3
J B D E Etc
インデックスデータD3
J B D E H Etc
属性データD4
J B F G K L Etc
アプリケーション毎に独立に存在する
[記号の意味]
A:ヘッダ
B:許可結果
C:クライアントマシン名
D:ドメインユーザ名
E:パスワード
F:アプリケーション名
G:バージョン情報
H:サーバーコード
I:許可／拒否データ
J:テンバー
K:実行権限
L:属性
Etc:将来の拡張用エリア

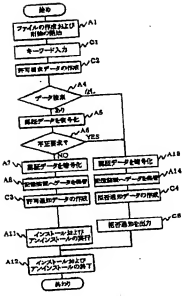
【図５】


[キー1]
ドメインユーザ名とパスワードが一致するデータを検索。
許可要求データD1
A B C D E F G Etc
インデックスデータD3
J B D E Etc
[キー2]
テンバーに格納されている値でD3とD4の属性データD4を検索
(例)テンバーが100の場合、
属性データのテンバーの先頭になっている。
インデックスデータD3
100 B D E Etc
J
属性データD4
038 B F G K L Etc
105 B F G K L Etc
101 B F G K L Etc
[キー3]
アプリケーション名とバージョン情報が一致するデータを検索。
許可要求データD1
A B C D E F G Etc
属性データD4
J B F G K L Etc
[記号の意味]
A:ヘッダ
B:許可結果
C:クライアントマシン名
D:ドメインユーザ名
E:パスワード
F:アプリケーション名
G:バージョン情報
H:サーバーコード
I:許可／拒否データ
J:テンバー
K:実行権限
L:属性
Etc:将来の拡張用エリア

【図７】


始め
インストールおよびアンインストールの指示
A1
キーワード入力
C1
許可署名データの作成
C2
データ検索
A4
YES
あり
既成データを暗号化
A5
平定署名
A6
YES
NO
既成データを暗号化
A7
既成データを暗号化
A18
A8
新規検索データを作成
A14
許可署名データの作成
C3
既存署名データの作成
C4
既存署名を出力
C5
インストールおよびアンインストールの実行
A11
インストールおよびアンインストールの終了
A12
終わり

【図８】


始め
ファイルの作成および初期の処理
A1
キーワード入力
C1
許可署名データの作成
C2
データ検索
A4
YES
あり
既成データを暗号化
A5
平定署名
A6
YES
NO
既成データを暗号化
A7
既成データを暗号化
A18
A8
新規検索データを作成
A14
許可署名データの作成
C3
既存署名データの作成
C4
既存署名を出力
C5
インストールおよびアンインストールの実行
A11
インストールおよびアンインストールの終了
A12
終わり